

TABLE OF CONTENTS

<u>SECTION</u>	<u>PAGE</u>
Section 3 Auxiliary Services	3-1
3.1 Regional Hub Design for Required Ancillary Equipment (RAE)	3-1
3.2 Commercial Cost Avoidance and Hybrid Routing Feature	3-3
3.3 UC Gateways	3-5
3.4 Interface to Emergency Response Systems	3-8
3.4.1 Enhanced 911 Interface.....	3-8
3.4.2 Mass Notification Warning System Interface.....	3-8
3.5 Other Auxiliary Services.....	3-9

LIST OF FIGURES

<u>FIGURE</u>		<u>PAGE</u>
Figure 3.1-1.	Regional RAE Hub Topology	3-2
Figure 3.2-1.	Hybrid Routing Feature Operation in the Network.....	3-4
Figure 3.2-2.	Commercial Cost Avoidance Feature Operation in the Network	3-5
Figure 3.3-1.	Centralized Connection to Commercial Voice Internet Service Providers (ISPs).....	3-6
Figure 3.3-2.	Centralized Secure Connection to Wireless Carriers	3-7
Figure 3.3-3.	Allied Network Interfaces	3-8

SECTION 3

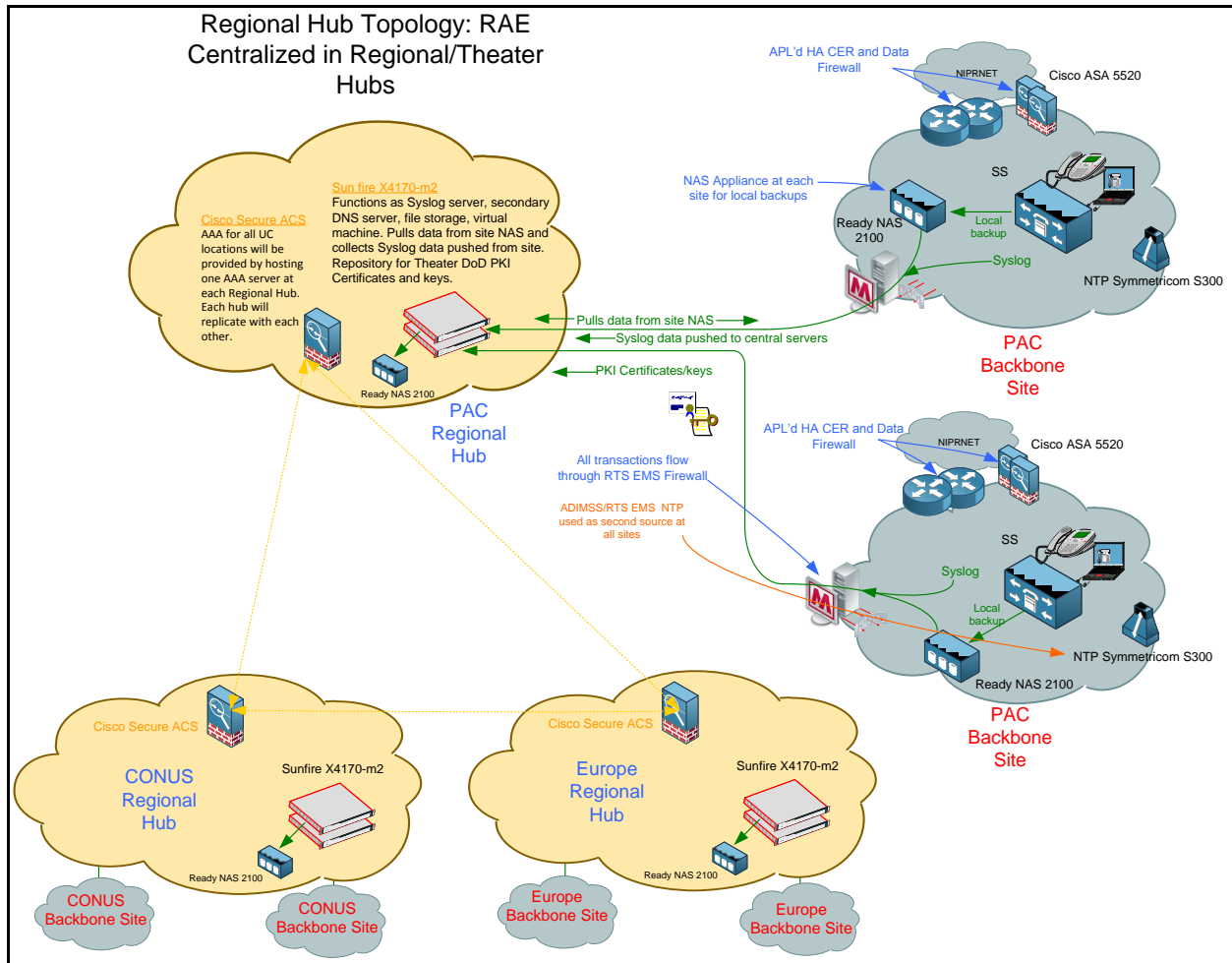
AUXILIARY SERVICES

This Section contains explanatory text on some of the Auxiliary Services Requirements in Unified Capabilities Requirements (UCR) 2013, Section 3, Auxiliary Services. It also contains explanatory text on other Auxiliary Services in the Unified Capabilities (UC) Network, including Services provided by Required Ancillary Equipment, and Services provided by UC Gateways (such as Centralized Connections to Commercial Voice Internet Service Providers, Centralized Secure Connections to Wireless Providers, and Allied Network Interfaces).

3.1 REGIONAL HUB DESIGN FOR REQUIRED ANCILLARY EQUIPMENT (RAE)

Operation of UC products requires management/security support from server functions that normally are not part of a Softswitch (SS), Session Controller (SC), or Session Border Controller (SBC) product. These functions/severs are referred to as Required Ancillary Equipment (RAE) and must be made available at the site to support the SS, SC and SBC. The RAE support includes Authentication, Authorization, and Accounting (AAA) servers; access to a Domain Name Service (DNS) server; SYSLOG server; Network Time Protocol (NTP) server; Dynamic Host Configuration Protocol (DHCP) server; and Department of Defense (DOD) Public Key Infrastructure (PKI) certificate verification, including access to an Online Certificate Status Protocol (OCSP) responder.

As a companion project associated with relocating SSs from a Military Department (MILDEP) to the Defense Information Systems Agency (DISA) network domain and security enclaves, DISA is in the process of procuring and installing RAE to support the SS nodes. To simplify management, minimize staffing and equipment cost centralized RAE hubs will be installed at Hickam, Scott, and Vaihingen. The three RAE hubs will provide support to the SSs within each theater. The RAE hub components will reside within the Defense Information Systems Network (DISN) network domain and DISA security enclaves. The operational concept for the regional RAE hub arrangement is illustrated in [Figure 3.1-1](#).



in User Server/Service (RADIUS) or Terminal Access Controller Access Control System (TACACS).

Additionally, the ACS servers will be configured to replicate with the other regional ACS servers located at the two other hub locations.

- b. Centralized Services will be provided to support off-site system backup storage, SYSLOG, secondary DNS service, and storage of Internet Protocol Detail Record's (IPDR) will be provided centrally by a server located at each regional hub. The centralized services will be provided by two Oracle Sun Fire X4170-m2 servers, one active and one backup.

3.2 COMMERCIAL COST AVOIDANCE AND HYBRID ROUTING FEATURE

The RTS Routing Database (DB) is a DISA-owned and DISA-operated DB that contains records of the Defense Switched Network (DSN) numbers, commercial [Public Switched Telephone Network (PSTN)] numbers, SC identifiers, and SS identifiers for UC end users served by SCs. This DB may also contain records of DSN numbers and commercial numbers for individual DSN end users served by DSN End Offices (EOs) and Private Branch Exchanges (PBXs). The DB records may be populated automatically by SCs, whenever end users' numbers are added to an SC during activation of that end user on the SC. The DB records also may be populated manually by a DISA craftsperson, using DSN and commercial number information from an SC site or DSN EO or PBX site.

The SSs that support the Hybrid Routing (HR) feature query the RTS Routing DB to determine whether there is an SC identifier, a primary SS identifier, and a backup SS identifier stored there that matches the dialed DSN number on a UC call that enters the SS. [Figure 3.2-1](#), Hybrid Routing Feature Operation in the Network, illustrates how the Hybrid Routing Feature operates in the network.

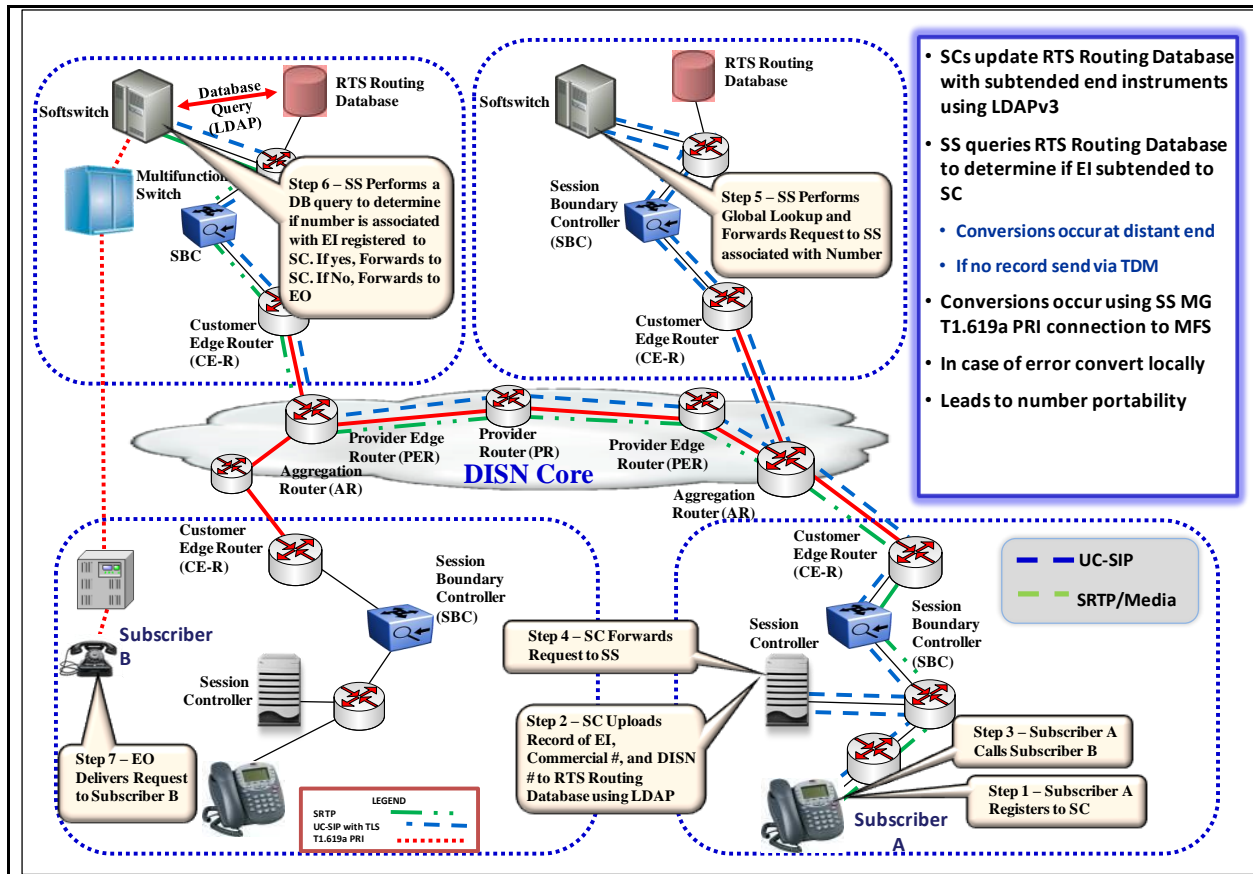


Figure 3.2-1. Hybrid Routing Feature Operation in the Network

The SCs that support the Commercial Cost Avoidance feature query the RTS Routing DB to determine whether there is a DSN number stored there that matches the dialed commercial number on a commercial call from the SC (e.g., a 9+9 call, or a 9+8 call). [Figure 3.2-2](#), Commercial Cost Avoidance Feature Operation in the Network, depicts how the Commercial Cost Avoidance feature operates in the network.

The protocol that SCs and SSs use to query and update the RTS Routing DB is Lightweight Directory Access Protocol (LDAP) version 3 (LDAPv3), secured using Transport Layer Security (TLS), and signaled via IP over the DISN Wide Area Network (WAN).

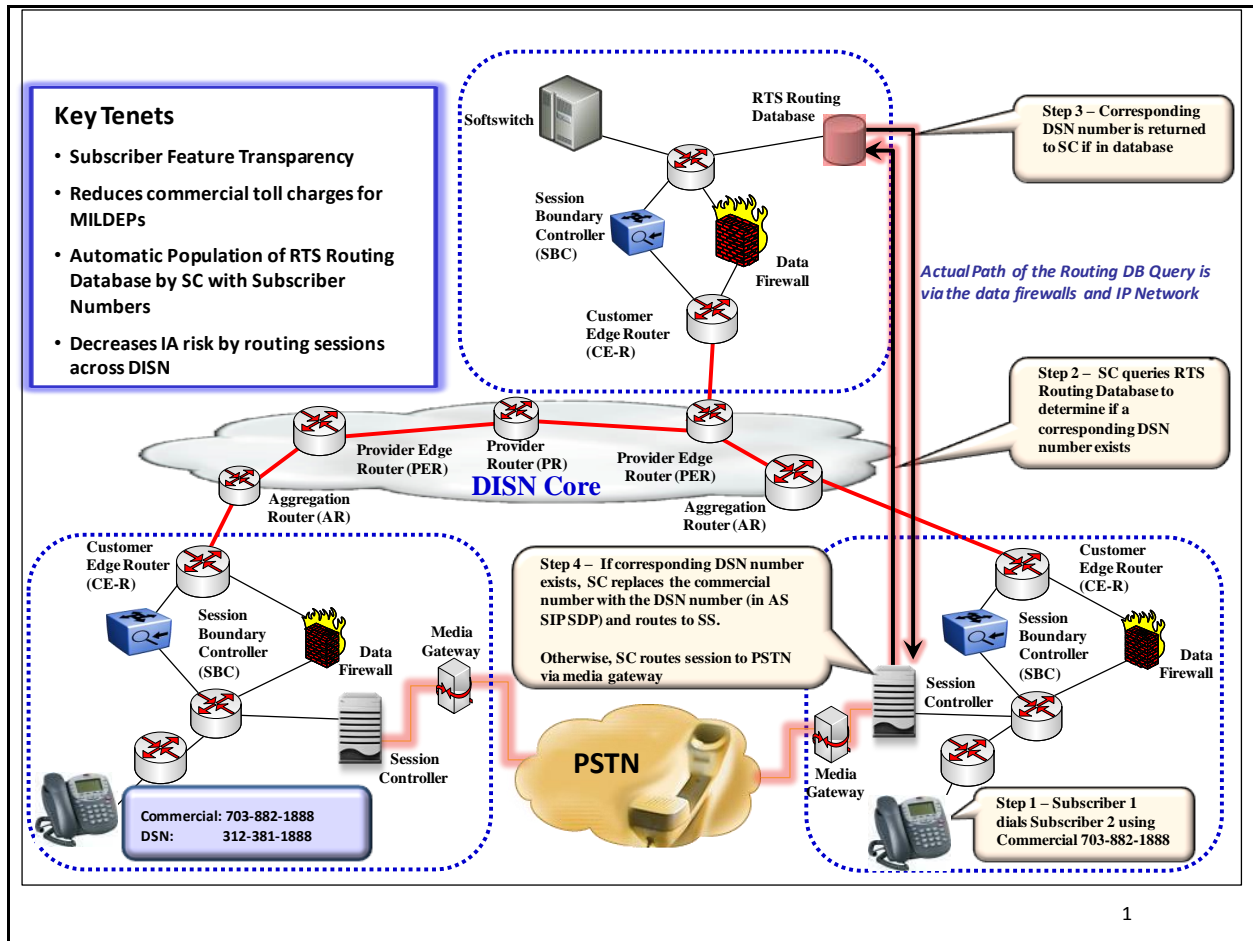


Figure 3.2-2. Commercial Cost Avoidance Feature Operation in the Network

3.3 UC GATEWAYS

As UC IP based products are deployed, a variety of gateways are necessary to interface non-DOD networks securely. These networks involve commercial public networks and Allied networks. Currently UC products will be employed in a variety of interfaces situations to non DOD networks as follows:

1. Centralized Secure Connection to Commercial Voice Internet Service Provider (ISP), as illustrated in [Figure 3.3-1](#).
2. Centralized Secure Connection to Wireless Carriers, as illustrated in [Figure 3.3-2](#).
3. Allied Networks Interfaces, as illustrated in [Figure 3.3-3](#).
4. Distributed “Authenticated/protected” UC Internet gateway to Trusted Voice/Video Networks [e.g., non-mission critical sites with no Non-Secure IP Router (NIPR) but with Internet Access to Centralized Connection to Commercial Voice ISPs (Item 1, above)].
5. Access to Internet, unauthenticated, untrusted networks employing Analog as opposed to digital interfaces.

[Figure 3.3-1](#), Centralized Secure Connection to Commercial Voice Internet Service Providers (ISP), depicts Centralized Secure Connection to Commercial Voice Internet Service Providers for allowing the user of an end instrument, in this case a softphone, to access the services provided by a Voice IP Service Provider (Voice ISP) from the MILDEP enclave. In this instance, session establishment and tear down signaling (the UC Session Initiation Protocol) is transported through enclave Session Border Controllers (SBCs) to an Enterprise SC which is co-located with an SS.

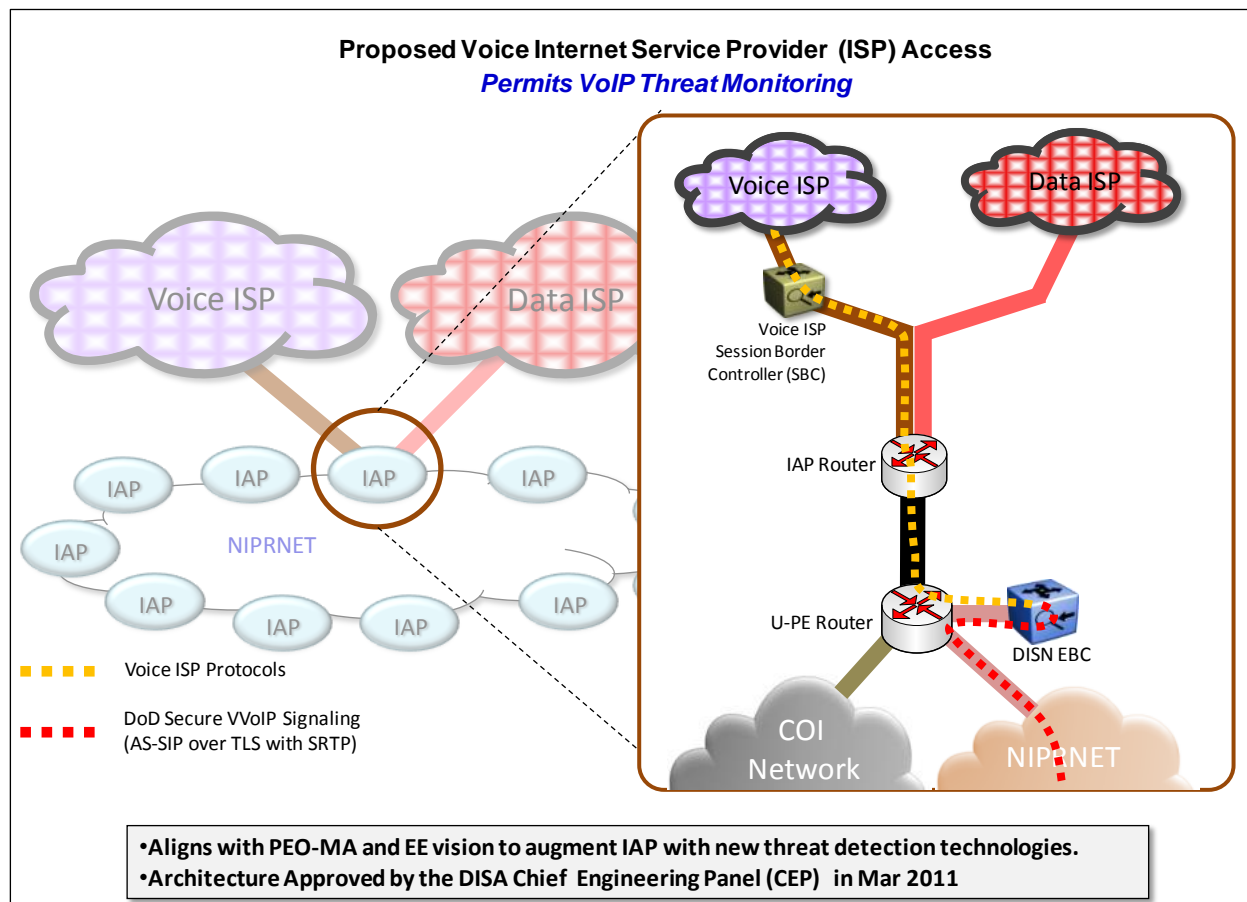


Figure 3.3-1. Centralized Connection to Commercial Voice Internet Service Providers (ISPs)

The signaling is forwarded to the Voice ISP's network once the call is determined to be for a PSTN destination or a destination serviced exclusively by the Voice ISP's network. Media traffic is transmitted directly between DISN SBCs across the DISN core. Within the Internet Access Point (IAP), the DISN SBC fronting the Voice ISP's network converts the signaling and media traffic streams into a format supported by the Voice ISP's SBC. It is anticipated that the interface between the commercial SBC and the DISN SBC at the IAP will be a commercial variant of Session Initiation Protocol (SIP) and Real-Time Transport Protocol (RTP).

The traffic between the Voice ISP's SBC and the DISN SBC in the IAP will be unencrypted, but authenticated, to allow monitoring and inspection by information assurance tools deployed at the IAP boundary.

[Figure 3.3-2](#) illustrates “Centralized Secure Connection to Wireless Carriers”. The multi-carrier entry point (MCEP) is a centralized access point for the wireless and cellular carriers to enter the DISN. DISA has several initiatives under way with the National Security Agency (NSA) and the carriers to increase support of mobility within the DOD by leveraging commercial wireless networks. The first effort is associated with a pilot undertaken within the NSA “Fishbowl” lab to evaluate a Mobile Virtual Network Operator (MVNO) concept, which is designed to replace the Secure Mobile Environment Portable Electronic Device (SME-PED) functionality as the SME-PED solution is phased out. The second effort is to allow Multifunction Mobile Device (MMD) applications to be installed on commercial MMDs and to allow those devices (such as Smartphones) to be connected to the DISN in a secure approach that is endorsed by the Security Technical Implementation Guidelines (STIGs) and the UCR. This aligns with U.S. Navy, Army, and Air Force initiatives to issue MMDs to warfighters as their primary end instrument. Finally, extension of the DISN to authorized commercial wireless and cellular end instruments, so they can transmit and receive DISN Sensitive but Unclassified (SBU) voice sessions from their commercial wireless or cellular end instrument, is being assessed.

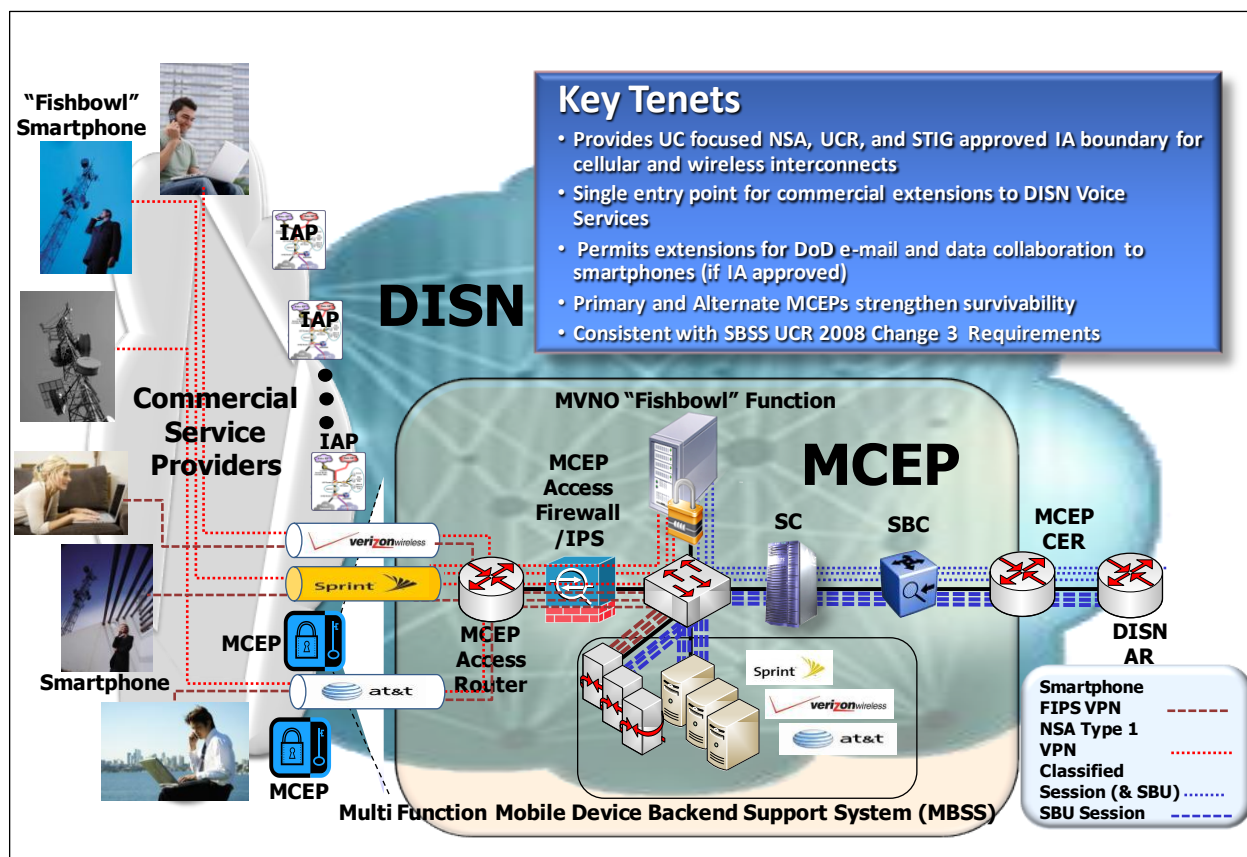


Figure 3.3-2. Centralized Secure Connection to Wireless Carriers

Figure 3.3-3 provides a high-level illustration of an interface to Allied networks.

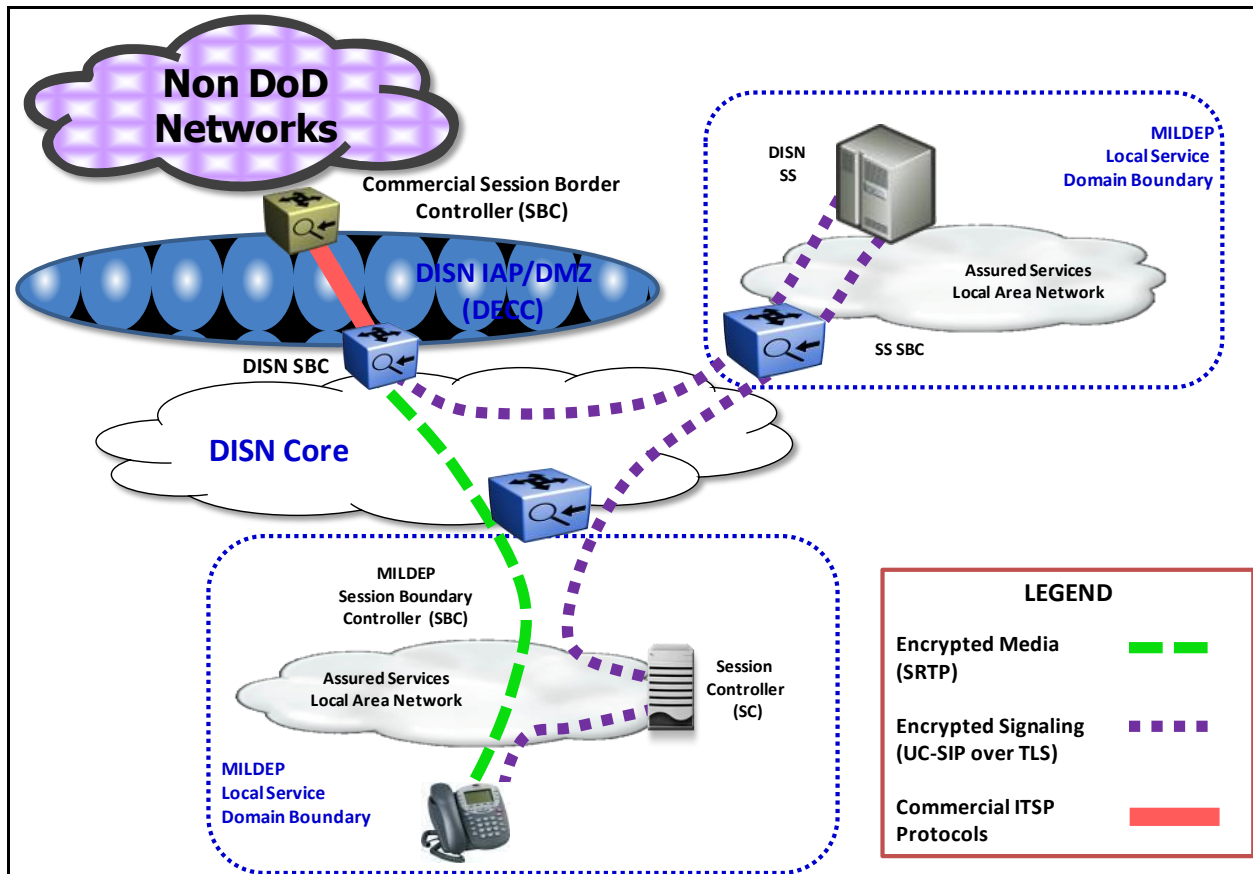


Figure 3.3-3. Allied Network Interfaces

3.4 INTERFACE TO EMERGENCY RESPONSE SYSTEMS

This section addresses two emergency response products that must be supported at DOD locations and must interface DOD UC products. These two systems are the E911 Management System and the Mass Notification Warning System.

3.4.1 Enhanced 911 Interface

Access to Enhanced 911 is available from SC/Media Gateways using the dial plan. This interface is Time Division Multiplexing (TDM) because of Information Assurance requirements. E911 Management Systems interface with SCs to provide reliable user locations to Public Safety Answering Points (PSAPs), including cases where DOD components host a PSAP for E911 services.

3.4.2 Mass Notification Warning System Interface

The Mass Notification Warning System will be used to meet the DOD's requirements to provide Association of Public-Safety Communications Officials (APCO) – International, Project 25,

systems at DOD locations. The Mass Notification Warning System is a product that monitors event sources and if an event from an event source meets pre-defined emergency criteria then the default action is for the Mass Notification Warning System (MNWS) to inform system operators of the event. The operators qualify the event and when appropriate instructs the system to initiate alerts. The system then initiates alerts via interfaces to alert delivery systems.

Currently all local access to any public network such as PSTN service; E911; and APCO – International, Project 25, systems must be via TDM and cannot be transmitted over IP, because of Information Assurance requirements. The only connection to the PSTN is through a TDM interface using Primary Rate Interface (PRI) or Channel Associated Signaling (CAS), so there is no interaction between the Voice and Video over IP (VVoIP) system and commercial VVoIP IP networks.

3.5 OTHER AUXILIARY SERVICES

Other auxiliary services that are included in UCR 2013 are as follows:

- UC audio and video conferencing systems.
- Customer premises equipment.
- DOD secure communications devices.